FARMINGTON POLICE DEPARTMENT

POLICY AND PROCEDURE

Policy Number:	Effective Date:
382-03	11/11/2016
Subject: Computer System Security	
Approved by: **Steven D. Hebbe, Chief of Police**	

PURPOSE:

To establish security procedures for the central records computer system.

POLICY:

It is the policy of the Farmington Police Department to establish security procedures designed to ensure the integrity of the central records computer system.

PROCEDURE:

Information Services:

The City of Farmington Information Services Department manages the central computer system. This includes system security and system backup. Daily system tape backups are performed automatically at midnight Monday through Friday for all programs, files and the NT server. Weekly backups are performed on Saturday including a Server Save backup of NT storage space and directory paths. Monthly a Save System backup is performed for control files and user profiles.

Backup tapes are stored off-site at the Farmington Fire Department main station in a fireproof safe. Daily backup tapes are stored for 33 days, NT server backup tapes for 12 months, Save System backup tapes for three months, and NT storage space backup tapes for three weeks. Tapes are recycled, being erased before they are reused. They are also erased prior to disposal.

Several levels of security are built into the central computer system. When a new user is added to the system they are assigned a default password. The first time they log on the default password automatically expires and they are required to create their own new password. Annually the system automatically requires users to change their password prior to being able to log on. When this change is made the user cannot reuse any of their previous 32 passwords.

The Human Resources Department will notify the Information Services Department of employees whose employment has terminated. Information Services personnel then remove that employee's user code from the system

If a user attempts to log on with an incorrect password the system will not allow access. After the third consecutive unsuccessful attempt the system will shut down (vary off) the workstation being used. After

verifying whether the system activities were access violations or accidental, Information Services personnel must enable the system to reactivate (vary on) the workstation before the user can log on.

IT Supervisor:

The IT Supervisor manages the Department's central records computer system, including security regarding user profiles. The New World records management system has several security features built in. The user must first log on to the central computer system then must log on to the New World system with an individual user profile and password. The New World system also has a last changed user, a last changed date feature and a transaction audit capability for tracking activities in the system files.

On a monthly basis the IT Supervisor conducts an audit of the user profiles to ensure that user profiles listed in the system are current. On an annual basis the IT Supervisor requests a User Profile printout showing password expirations which is used to conduct an audit of user profiles, passwords and any access violations to ensure the integrity of the system. The IT Supervisor documents this annual audit by means of an inter-office memorandum.

Introduction of outside computer software and disks into the computer system, desktop or laptop workstations must first be authorized by the IT Supervisor.